



***Управление  
информационной  
безопасностью в среде  
виртуализации VMware***

*Текущее состояние, проблемы и  
перспективы развития*

**Мария Сидорова**

VMUG, Москва, 26 июня 2009

# Поговорим о...

- Плюсах и минусах документов по обеспечению информационной безопасности компании VMware;
- Проблемах, которые возникают при разработке концепций информационной безопасности для инфраструктуры виртуализации;
- Перспективах развития обеспечения информационной безопасности инфраструктуры виртуализации.

# Best-practice

- VMware Infrastructure 3.5 Security Hardening (VMware);
- VMware ESX server 3.x Benchmark (CIS);
- VMware ESX server in the Enterprise Planning and securing virtualization servers (Edvard L. Haletky);
- VMware Virtual Infrastructure3 Security Risk Assessment (Xtravirt).

# Экспресс-анализ ESX-серверов

**Configuresoft**

### Compliance Assessment Summary

Printable Version

Overall Compliance: **75%** 192.168.0.249 **75%**

- VMware Infrastructure 3 Security Hardening v2.0: **78%**
- CIS VMware ESX Server 3.x Benchmark: **73%**

Assessment Time: 06/26/09 10:54:42

#### VMware Infrastructure 3 Security Hardening v2.0

Center for Internet Security VMware ESX Server 3.x Benchmark

Key:	Passed Check	Failed Check	Unknown Status	Machine Not Found
Compliance Rule	192.168.0.249			
Configure syslogd to Send Logs to a Remote LogHost		✘		
Configure syslogd to Send Logs to a Remote LogHost - *.emerg		✘		
Configure syslogd to Send Logs to a Remote LogHost - *.err		✘		
Configure syslogd to Send Logs to a Remote LogHost - *.info		✘		
Configure syslogd to Send Logs to a Remote LogHost - local2.*		✘		
Configure syslogd to Send Logs to a Remote LogHost - local7.*		✘		
Configure the Service Console Firewall for High Security	✔			
Configure the Service Console Firewall for High Security: Authentication Traffic	✔			
Configure the Service Console Firewall for High Security: CIM Secure Server	✔			
Configure the Service Console Firewall for High Security: CIM SLP	✔			
Configure the Service Console Firewall for High Security: DHCP	✔			

**Tripwire ConfigCheck**

About

VMware CONFIGCHECK

ESX Hostname: 192.168.0.249 Username: nem0  
Password: \*\*\*\*\* Root Password: \*\*\*\*\* Check Configuration

Check Complete: **40 Passed, 37 Failed**

#### Checking ESX host: 192.168.0.249

Vendor Guides

VMware Infrastructure 3 Security Hardening - ESX 3.5

- Virtual Machine Files and Settings
  - 1.1 Disable Copy and Paste Operations between the Guest OS and Remote Console
    - 1.1.1 Verify Copy Is Disabled between Guest OS and Remote Console **Failed**
    - 1.1.2 Verify Paste Is Disabled between Guest OS and Remote Console **Failed**
    - 1.1.3 Verify Option to Override VMware Tools Settings Is Disabled **Failed**
  - 1.2 Limit Data Flow from the Virtual Machine to the ESX Server Host
    - 1.2.1 Verify Log Rotate Size for Virtual Machines Is <= 100KB **Failed**
    - 1.2.2 Verify the Number of Log Files to Keep Is Equal to 10 **Failed**
    - 1.2.3 Verify Size of GuestInfo File Is <= 1MB **Failed**

Additional Information for Tripwire ConfigCheck (TM):  
[Privacy Policy](#) [Support FAQ](#)  
[End User License Agreement](#) [VMware Infrastructure 3 Security Hardening](#)

MONITOR CORRELATE ACT

Take control of your virtual infrastructure. Discover vWire for yourself.

DOWNLOAD FREE TRIAL

# Уровни безопасности

- Уровень виртуализации (VMKernel и монитор виртуальной машины);
- Виртуальные машины;
- Сервисная консоль сервера ESX;
- Сервер ESX (уровень виртуальной сети);
- Сеть хранения данных;
- Сервер управления инфраструктурой Virtual Center.

VMware Virtual Infrastructure3 Security Risk Assessment (Xtravirt).

# Реагирование на инциденты

- Скомпрометирована виртуальная машина;
- Скомпрометирован отдельный сервер ESX;
- Скомпрометирован ESX сервер кластера;
- Скомпрометирован Virtual Center.

# Перспективы развития

- Разработка продуктов и технологий обеспечения информационной безопасности инфраструктуры виртуализации;
- Консолидированные усилия специалистов и сообщества пользователей продуктов VMware, направленные на противодействие угрозам в среде виртуализации.

***Skype: m.e.sidorova***

***Email: sidorova@almitech.ru***

Мария Сидорова

Москва, 26 июня 2009

